

**UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF TEXAS
DEL RIO DIVISION**

UNITED STATES OF AMERICA,
Plaintiff,

v.

MICHAEL SCOTT MCAULEY,
Defendant.

§
§
§
§
§
§
§
§

DR-07-CR-786(1)-AML

ORDER

A hearing on the Defendant's Motions to Suppress Evidence (Docket Entries #30 and #33) in the above-styled case was held on January 4, 2008. Both parties were given time by the Court to file supplemental briefs which were received by January 24, 2008 (Docket Entries #40, #41, and #43). Having considered the motions, responses, and the evidence adduced at the hearing, the Court makes the following findings of fact and conclusions of law.

I. FINDINGS OF FACT

On August 28, 2007, at approximately 1:49 p.m., Defendant, Michael Scott McAuley, drove a 1999 Chevy Blazer into the primary inspection station at the Del Rio, Texas Port of Entry from the Republic of Mexico. The Defendant declared he was a United States citizen. Agents ran a name check on the Defendant and received information that he was the subject of an investigation for suspected criminal acts involving child pornography in New York. There were no outstanding warrants for his arrest, nor was he considered a fugitive. The Defendant was then referred to the secondary inspection area for further review and inspection.

Immigration and Customs Enforcement ("ICE") Agent Robert Mayer, Jr. was the duty agent

on August 28th.¹ At about 2:20 p.m., Agent Mayer was notified of the Defendant's earlier arrival at the port of entry. The agent arrived at the port of entry approximately 10-15 minutes later.

Prior to his arrival at the port of entry, Agent Mayer contacted an agent in New York seeking more information on the Defendant and the child pornography investigation.² When Agent Mayer arrived at the port of entry, he saw the Defendant had computer equipment in his vehicle consisting of a zip drive, two external hard drives, and a laptop. The Defendant also had camping gear.

The Defendant was sitting in an office at the port of entry from 2:40 until 3:30 p.m. No formal questioning of the Defendant had taken place during this time period. The Defendant's computer and external drives were also not searched during this same time period.

Agent Mayer first conversed with the Defendant around 3:30 or 3:45 p.m. Agent Mayer testified that he had a conversation with the Defendant regarding his trip to Mexico. The Defendant stated he was on his way to California for an employment opportunity when he made a wrong turn and ended up crossing the border into Mexico. The Defendant was then asked if the computer in his possession was his personal laptop, to which the Defendant replied it was. Agent Mayer asked for, and received, verbal consent from the Defendant to search the laptop. Agent Mayer stated that he asked for consent so as not to appear as if bullying the Defendant. No threats or false promises were

¹ Agent Mayer has been an ICE Agent since November 2002, and previously worked as an investigator for the Val Verde County Sheriff's Office, and was assigned to the DEA task force.

² There was some dispute as to whether the agent in New York specifically told Agent Mayer to detain the Defendant and search his computer. Agent Mayer testified that he did not recall having this particular conversation with the New York agent, however, Agent Mayer stated that the Defendant's computer would have been searched regardless because of the information that appeared from the Defendant's name query, and that most people cannot leave the inspection area until the search of their items has been completed.

used to coerce the Defendant into giving consent.

ICE Agent Olsteen was also present with Agent Mayer during the questioning of the Defendant. After obtaining verbal consent to search the computer, the agents realized they did not have a written consent form with them. They called the Del Rio ICE Office to have a consent form sent to them at the port of entry via telefax. While the agents were waiting, Agent Olsteen hooked up the laptop and turned on the power. A password was needed to gain access to the computer and the Defendant was asked for the password. The Defendant voluntarily gave the agents the password, which was "1969."

Agent Olsteen proceeded to search the computer and did not find any explicit materials in the files. Agent Olsteen then began examining the external hard drives using the Defendant's laptop.³ Agent Mayer, in the meantime, received the consent form over the telefax machine and listed the items to be searched on the form. Agent Mayer read the consent form to the Defendant at 4:09 p.m., but the Defendant replied that he "would rather not sign the form." However, the Defendant never withdrew his verbal consent to the search of the computer and computer equipment.

As Agent Olsteen was searching an external hard drive, he discovered pornographic images depicting children and ceased his search to have the files analyzed by another agent. From the beginning of the search to the time pornographic images were uncovered, approximately 40 minutes of time had elapsed. Once the images were found by the agents, the Defendant was advised of his constitutional rights per *Miranda v. Arizona*, 384 U.S. 436 (1966). The Defendant stated he understood his rights and signed the rights form. The Defendant asked for an attorney. All

³ Agent Mayer testified that there were computers at the port of entry and Agent Olsteen would have been able to access the hard drives from any of these computers without the need of the Defendant's laptop which was password protected.

questioning of the Defendant was ceased.

Agents ultimately found 101,000 still images depicting child pornography, of which 1,688 were considered hardcore pornography, on an external drive. The agents also uncovered 890 videos depicting pornographic images of children, of which 381 were considered to be hardcore pornography, on the same external drive.

The Defendant testified at the suppression hearing claiming that the day he was arrested, he had gone to Mexico around 1:30 p.m. and was there for approximately half an hour before returning to the United States. The Defendant is an electrician by trade and was traveling from New York to California under a union travel option to obtain work. The Defendant would stay at campsites during his travels, and on this particular trip, he had decided to take Highway 90 instead of Interstate Highway 10 because he believed he could see the border and the border fence. The Defendant claimed to have made a wrong turn while driving, not seeing any signs advising he had crossed into Mexico, and mistakenly ended up in Mexico.⁴ When he re-entered the United States, he was sent from primary to the secondary inspection area where he was asked to step out of his vehicle so it could be searched. The Defendant claims the agents did not search his bags at that time, but generally looked around his vehicle, which he thought was extreme considering he was a citizen returning to the country. He was then asked to wait in an office and claims he was there for well over an hour before speaking with Agent Mayer. According to the Defendant, he was asked by Agent Mayer where his parents lived, some general background information to confirm his citizenship, and about the computer found in the vehicle. The Defendant replied that he owned the

⁴ The controversial border fence has not been erected in Del Rio, Texas. Additionally, the Defendant would have had to stop at a toll booth and paid a toll to cross the international bridge into Mexico.

computer and the vehicle, as well as the hard drives and all personal belongings in the vehicle.

The Defendant then testified that he never verbally consented to the search of his computer prior to giving the agents his password. He claimed he did not want his personal items searched. The Defendant contends he asked for a lawyer when he received the consent form, although he admits to giving agents his password prior to asking for an attorney. The Defendant testified that Agent Mayer informed him that he did not need a warrant to search and he did not have a choice in the matter because he was detained.⁵

II. CONCLUSIONS OF LAW

The Court finds the Defendant has standing to contest his seizure and the seizure and search of the vehicle and its contents. The Fourth Amendment guarantees “the right of the people to be secure in their persons...and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause...” U.S. CONST. amend. IV. “Warrantless searches and seizures are per se unreasonable unless they fall within a few narrowly defined exceptions.” *United States v. Roberts*, 274 F.3d 1007, 1011 (5th Cir. 2001) (quoting *United States v. Cardenas*, 9 F.3d 1139, 1147 (5th Cir. 1993)).

An international border, such as the port of entry in the present case, is one exception which requires a qualitatively different analysis under the Fourth Amendment. *United States v. Montoya de Hernandez*, 473 U.S. 531, 538 (1985). The Fourth Amendment’s balancing test of interests leans

⁵ The Court believes Agent Mayer to be a credible witness and relies on his testimony. The Court had a difficult time ascertaining the truth of the Defendant’s testimony at the hearing. While the Court believes some of the Defendant’s statements, the Court affords little weight to his testimony. The Court had an especially difficult time believing the Defendant made wrong turns, which inadvertently, took the Defendant to Mexico without his perceiving a border check station or signs of crossing the international boundary.

heavily toward the Government at international borders. *United States v. Ramsey*, 431 U.S. 606, 619 (1977). “Routine searches of the persons and effects of entrants [into the United States] are not subject to any requirement of reasonable suspicion, probable cause, or warrant...” *Id.* Pursuant to this long-standing border search doctrine, the Court finds that the search of the Defendant’s vehicle and personal items was lawful pursuant to the Fourth Amendment.

The Defendant specifically contends that the search of his personal computer should be considered a non-routine search and, thus, the Government must prove the agents had reasonable suspicion or probable cause to search it. (Def. Amended Mot. to Supp., 4-5.) He also claims the images and videos found on the external drive should be suppressed as “fruits of a poisonous tree” per *Wong Sun v. United States*, 317 U.S. 471 (1963). (Def.’s Brief, 7.)

A. Legality of the Search and Seizure

1. The Border Search Doctrine

Automotive travelers and other persons entering the United States may be stopped at fixed points along the international borders without any individualized suspicion. *Montoya de Hernandez*, 473 U.S. at 538. To protect the territorial integrity of this country, courts have made it clear that each person entering into the United States must be prepared to identify himself as entitled to enter and establish the right to bring in his effects. *Carroll v. United States*, 267 U.S. 132, 154 (1925).

The border search doctrine is one of the few exceptions that allow a warrantless search at a port of entry. “Agents may conduct a ‘routine’ search—one that does not seriously invade a traveler’s privacy at the international border or its functional equivalent without probable cause, a warrant, or any suspicion to justify the search.” *Roberts*, 274 F.3d at 1011 (internal quotations and citations omitted). The key variable used to determine whether a search is “routine” is “the invasion of the

privacy and dignity of the individual.” *United States v. Sandler*, 644 F.2d 1163, 1167 (5th Cir. 1981). The Fifth Circuit has determined that ordinary pat-downs and frisks, removal of outer garments and shoes, and the emptying of pockets, wallets, and purses are all routine searches, which “require no justification other than the person’s decision to cross our national boundary.” *Id.* at 1169.

The United States Supreme Court considered the issue of a routine border search in the context of the search of a car’s fuel tank. *United States v. Flores-Montano*, 541 U.S. 149 (2004). Chief Justice Rehnquist, writing for the Court, stated that “[c]omplex balancing tests to determine what is a ‘routine’ search of a vehicle, as opposed to a more ‘intrusive’ search of a person, **have no place** in border searches of vehicles.” *Id.* at 152 (emphasis added). He reasoned that the

Government’s interests in preventing the entry of unwanted people and effects is at its zenith at the international border. Time and again, we have stated that “searches made at the border, pursuant to the longstanding right of the sovereign to protect itself by stopping and examining persons and property crossing into this country, **are reasonable simply by virtue of the fact that they occur at the border.**”

Id. at 152-53 (quoting *Ramsey*, 431 U.S. at 616) (emphasis added).

A non-routine search requires ““reasonable suspicion of wrongdoing to pass constitutional muster.”” *United States v. Rivas*, 157 F.3d 364, 367 (5th Cir. 1998) (quoting *Cardenas*, 9 F.3d at 1148 n. 3). “Reasonable suspicion of criminal activity must be based upon ‘specific facts which, taken together with rational inferences therefrom, reasonably warrant an intrusion’” into someone’s privacy. *Id.* (quoting *Cardenas*, 9 F.3d at 1153). An agent must have “a particularized and objective basis for suspecting the particular person” of smuggling contraband in order to possess the requisite reasonable suspicion for a “non-routine” search. *Montoya de Hernandez*, 473 U.S. at 541 (internal

quotations and cites omitted). The Fifth Circuit has held that body cavity searches, strip searches, and X-rays of a person are all non-routine searches. *Sandler*, 644 F.2d at 1166. Searches such as these are likely to trigger significant embarrassment for any person, and invade “the privacy and dignity of the individual.” *Id.* at 1167.

The Defendant would like the Court to believe that the search of his computer was unauthorized because he maintains a higher degree of privacy in his computer, due to the personal nature of information contained therein. The Defendant claims that any search of a computer is akin to a bodily search of a person and should be categorized as a non-routine search requiring a finding of reasonable suspicion in order to conduct such a search. The Defendant would have this Court impute the same level of privacy and dignity afforded to the sovereignty of a person’s being to an inanimate object like a computer. The Court finds this argument without merit. Relying on the Supreme Court’s reasoning in *Flores-Montano*, this Court cannot equate the search of a computer with the search of a person. The Court finds that the search of a computer is more analogous to the search of a vehicle and/or its contents.

Travelers crossing an international border checkpoint should reasonably expect to be stopped and possibly searched with regard to any items on their person, or belongings they are transporting. Persons bringing their personal computers across our border are not exceptions to this rule simply because their computers may contain personal information. Since “a ‘port of entry is not a traveler’s home,’ his expectation of privacy there is substantially lessened.” *United States v. Ickes*, 393 F.3d 501, 506 (4th Cir. 2005) (quoting *United States v. Thirty-Seven Photographs*, 402 U.S. 363, 376 (1971)). Although relying on 19 U.S.C. § 1581(a), the *Ickes* court refused to find that reasonable suspicion or probable cause are a prerequisite to a search of personal computers and disks. *See Id.*

at 507-08.

The Defendant believes that a search of the computer is much more intrusive than ordinary searches at ports of entry because of the type of information available on a computer. (Def. Amended Mot. to Supp., 4.) The Court is not persuaded by this contention. Incredible amounts of personal and sensitive information are already subject to scrutiny at ports of entry in peoples' wallets, purses, locked glove boxes, and locked containers or luggage. People carry personal items such as Social Security cards; state and federal identification cards; medicines and medical records; names and addresses of family and associates; day planners with itineraries and travel documents; credit cards; check books and registries; business cards; photographs; and membership cards. All of these items are already subject to routine border searches. *See Cardenas*, 9 F.3d at 1148 n. 3. A computer is simply an inanimate object made up of microprocessors and wires which happens to efficiently condense and digitize the information reflected by the items listed above. The fact that a computer may take such personal information and digitize it does not alter the Court's analysis.

While the Defendant's computer was password protected, it too does not effect this Court's analysis. A password on a computer does not automatically convert a routine search into a non-routine search. A password is simply a digital lock.⁶ Locks are usually present on luggage and briefcases, yet those items are subject to "routine" searches at ports of entry all the time. *See Flores-Montano*, 541 U.S. at 154-55.

In this particular case, the Defendant was transporting his personal laptop and related equipment in his vehicle across the border through an international port of entry. The agents were

⁶ The Defendant's computer was password protected. However, the external drive containing the pornographic images and videos was not so protected. Arguably, the external drive was not "locked."

well within the legal parameters of the border search doctrine, which gave them the authority to search personal items in the Defendant's vehicle without reasonable suspicion, probable cause or a warrant. Although the Court believes the name check did lead agents to become suspicious⁷ of the Defendant, agents at the port of entry had authority to search the computer and all of his belongings regardless of the status of the New York investigation. It is inconsequential if agents in New York did or did not request a search of the Defendant due to their ongoing investigation because a warrant or probable cause is not needed to search when crossing the border at a port of entry. The Defendant's claim of "surprise" should not be a basis to disallow agents from searching any items in the Defendant's vehicle. He did, after all, cross into a foreign country and attempt to re-enter the United States.

A search of items like a computer, unlike a strip search of a person, is not per se embarrassing. Although not required, the search of the Defendant's computer and related equipment took place in a room away from the busy port of entry inspection lanes, which was free from the public's scrutiny, and that did not attract unnecessary attention to the Defendant. They were in a location out of the general public's view when the pornographic images were found on the external drive. The search was not conducted in an open and public inspection area where anyone passing by could have seen the pornographic pictures and associate those with the Defendant causing him significant embarrassment.

This Court finds that the search of one's personal computer at a port of entry is a routine

⁷ While the Court does not decide whether the agents actually had reasonable suspicion to search the computer equipment at this time because it believes reasonable suspicion is not needed in this case, the name check information coupled with the presence and amount of computer equipment the Defendant had is arguably sufficient information to determine the existence of reasonable suspicion to search.

search and thus, does not necessitate a finding of reasonable suspicion in order to search a computer, disks, hard drives, or any other technical devices.

2. Statutory Authority to Search

Although the Court has found that the search in this case was legal under the border search doctrine, the following alternative findings leading to the same conclusion are made to further the resolution of the issues.

In addition to the permissible search discussed above, the agents were also authorized to search a vehicle's contents under statutory authority. 19 U.S.C. § 1581(a) provides in pertinent part:

Any officer of the customs may at any time go on board of any vessel or vehicle at any place in the United States...or at any other authorized place...and examine the manifest and other documents and papers and examine, inspect, and search the vessel or vehicle and every part thereof and *any person, trunk, package, or cargo on board...* (emphasis added).

“Congress, since the beginning of our Government, ‘has granted the Executive plenary authority to conduct routine searches and seizures at the border, without probable cause or a warrant, in order to regulate the collection of duties and to prevent the introduction of contraband into this country.’” *Flores-Montano*, 541 U.S. at 153 (quoting *Montoya de Hernandez*, 473 U.S. at 537).

It is undisputed that the Defendant’s computer and hard drives were transported by his vehicle across the border through the port of entry. This statute clearly gives authority to agents, especially at a port of entry, to search a vehicle and any of its cargo. The Defendant’s computer, hard drives, and any other belongings being transported in the Defendant’s vehicle would clearly be classified as cargo and subject to a search under this statute. *See Ickes*, 393 F.3d at 506.

3. Consent

During the search of the actual computer, the agents asked for and received verbal consent

from the Defendant to search the computer. Although not a legal necessity since verbal consent was obtained, the agents took steps to obtain a written consent form. They made arrangements to obtain one as they conducted the search of the computer. The agents obtained the Defendant's computer password, which he freely provided, to access the computer files while awaiting receipt of the written consent form. When the Defendant was presented with the written consent form, he refused to sign the form. The Defendant argues that this refusal to sign revoked his consent. The Government argues that consent was never needed because the search took place at a port of entry.

"Consent operates as a waiver of Fourth Amendment rights if, by a preponderance of the evidence, it is found to have been given voluntarily under the totality of the circumstances." *United States v. Webster*, 162 F.3d 308, 333 (5th Cir. 1998). "Consent must be given voluntarily and not simply in acquiescence to a claim of lawful authority." *Schneckloth v. Bustamonte*, 412 U.S. 218, 248 (1973). A court should determine the voluntariness of consent by considering the totality of circumstances, in light of the following six factors: (1) the defendant's custodial status; (2) the presence of coercive law enforcement procedures; (3) the extent and level of the defendant's cooperation with law enforcement; (4) the defendant's awareness of his right to refuse to consent; (5) the defendant's education and intelligence; and (6) the defendant's belief that no incriminating evidence will be found. *United States v. Cooper*, 43 F.3d 140, 144 (5th Cir. 1995). No single factor determines voluntariness, and the Government bears the burden of proving that consent to search was voluntarily given. *See Id.*

Agent Mayer asked the Defendant for consent to search his computer to avoid the appearance of bullying the Defendant. No threats, coercive tactics, or promises were used to force the Defendant into giving consent. The Defendant was not under any type of custodial detention or formal arrest

at the time consent was requested. The Defendant was free to leave, however, Agent Mayer did testify that most people will not leave until the agents at a port of entry complete their searches. The Defendant demonstrated that he was educated and intelligent enough to work as an electrician by trade and is a member of a union in his profession.

The Defendant voluntarily gave the agents verbal consent to search his computer. The Defendant reaffirmed his verbal consent by cooperating with agents and freely providing the password to his computer to further the search of the computer. These acts by the Defendant further supports the Court's belief that the Defendant knew no incriminating evidence would be found on the laptop.

The Defendant's refusal to sign the consent form once it arrived does not automatically vitiate his verbal consent. Testimony shows that the pornographic images were not found until approximately 40 minutes after he refused to sign the written consent form. No evidence was presented by either party that during these 40 minutes the Defendant continually protested the search, requested that the search be stopped, or otherwise explicitly and affirmatively withdraw his consent to search. Consent was voluntarily given by the Defendant, and he did not rescind his verbal consent by refusing to sign the written consent form. *See United States v. Mata*, 517 F.3d 279, 291 (5th Cir. 2008) (finding that refusal to sign the written consent form did not constitute a withdrawal of verbal consent). The act of refusing to sign the consent form demonstrates to the Court that the Defendant was aware that he had a right to refuse consent if he wished. He exhibited a full understanding of his rights.

Based upon these findings and the totality of the circumstances, the Court finds the Defendant voluntarily gave verbal consent. Therefore, in the alternative, the searches of the

computer and computer equipment were constitutional due to the Defendant's voluntary consent to search.⁸

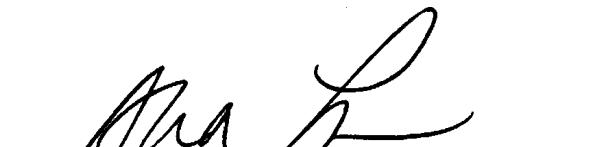
B. Evidence Obtained from a Border-Search and Fruit of the Poisonous Tree

Under the "fruit of the poisonous tree" doctrine, all evidence produced as a result of an illegal search or seizure must be suppressed, unless the Government can show that there was a break in the chain of events sufficient to refute the inference that the evidence was a product of the Fourth Amendment violation. *Wong Sun v. United States*, 371 U.S. 471, 484 (1963); *Brown v. Illinios*, 422 U.S. 590, 602-03 (1975). Because of the Court's findings and analyses of the border search and consent doctrines, a *Wong Sun* analysis is not necessary.

III. CONCLUSION

The Court finds that the seizure and searches of the Defendant's computer and related equipment were constitutional. All evidence obtained due to the searches are admissible at a trial on the merits. The Defendant's formal arrest resulting from the discovery of the child pornography is also constitutionally valid. Therefore, the Defendant's Motions to Suppress Evidence (Docket Entries #30 and 33) are **DENIED**.

SIGNED this 6th day of June, 2008.



ALIA MOSES LUDLUM
UNITED STATES DISTRICT JUDGE

⁸The Court finds it unnecessary, in light of the findings contained in this order, to engage in a discussion about the inevitable discovery doctrine argument raised by the Government.